

EXHIBIT F

Distributed Network Defense Systems



Strategic Overview

September 24, 2000

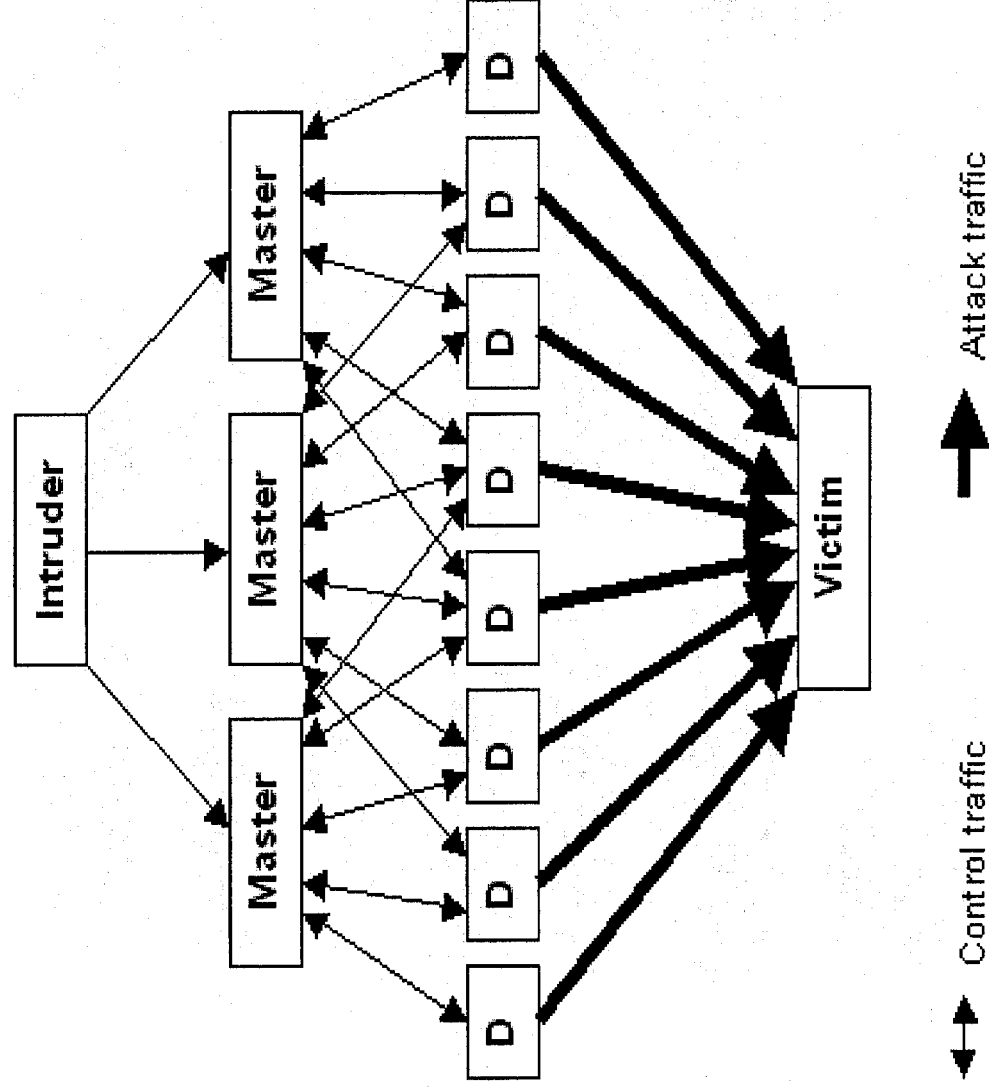
Net-guards

What is Distributed Denial of Service Attack (DDoS)? (*)

- Swamp victim & deny service from customers:
 - Exhaust resources
 - Jam routers, networks & discs....
- Distributed Attacks:
 - Many sources (daemons) bombardment
 - Master machines coordinate the attackers
- Several different versions in use: Trinoo, TFN, TFN2K and stacheldraht

EXHIBIT F

Distributed Denial of Service (*)



What is being done today?

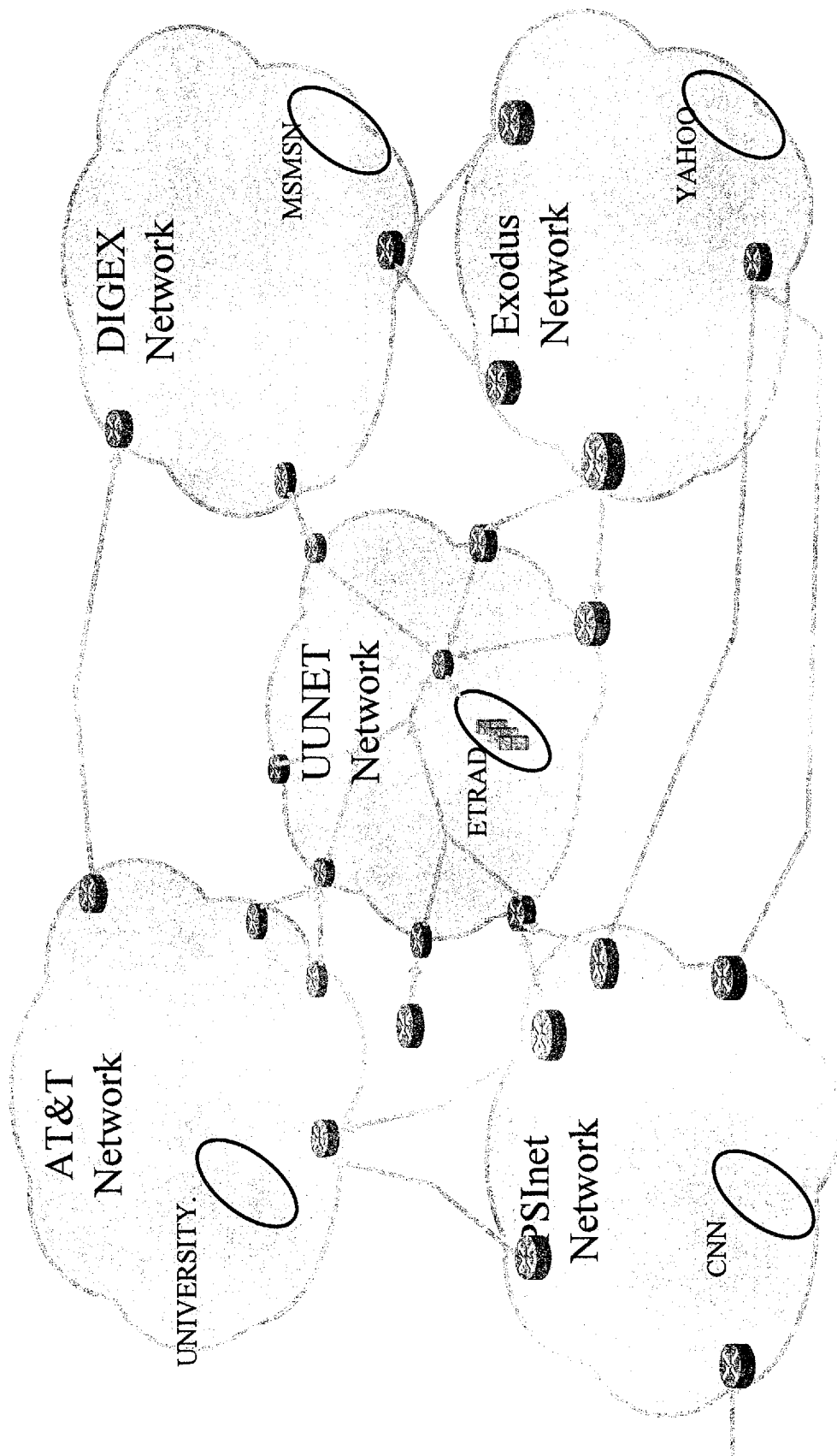
- Local on site:
 - Firewalls, IDSs, Router access lists, etc.
 - HOT SPOTS, congestion point
- Global network wide:
 - Ingress/Egress filtering and anti-spoofing
 - Anti virus scans
 - Turn off directed broadcasts
 - Enforcement problem \ Does not protect self

The Difficulties (*)

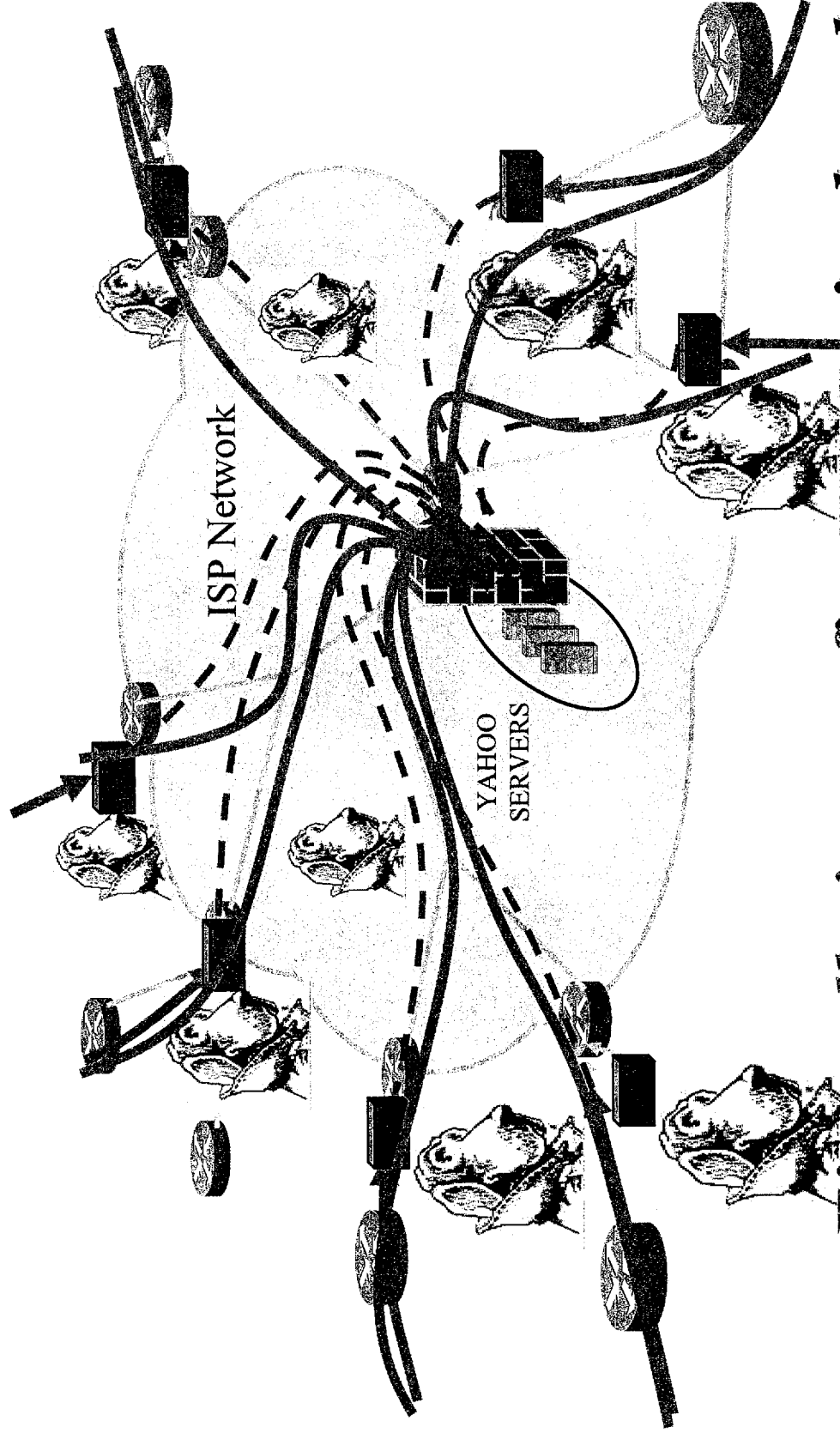
- Performance: Huge Capacity & Proc. Needs
- Defense resource not function of site size
- Solution cannot be in the site level
- "We have no real defense". Steve Bellovin

ATT Feb '00, David Dittrich WU, Aug '00

Internet structure



Solution is in the ^{EXHIBIT}AS level (ATT, exodus, digex, MCI, ...).



Disirevvald id eqanfre, e server is shut down

Solution Overview

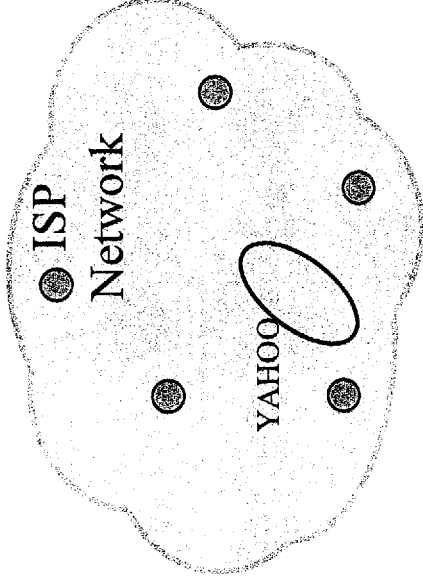
- Detect & Alert system in each site
- Alert invokes guards sitting around
- Divert victim traffic to guards
- Guards:
 - Anti spoofing module
 - Statistical module
 - Filtering module
 - Ingress filtering management
 - Distributed termination detection module

Core Technologies

- New concept for distributed defense
- Anti spoofing & Filtering
- Diversion method
- Experience in Protocols & Distributed Algs
- New programmable Network processors
(Intel IXP1200, Ezchip, Motorola, MMC, etc.)
- Provisional patent application

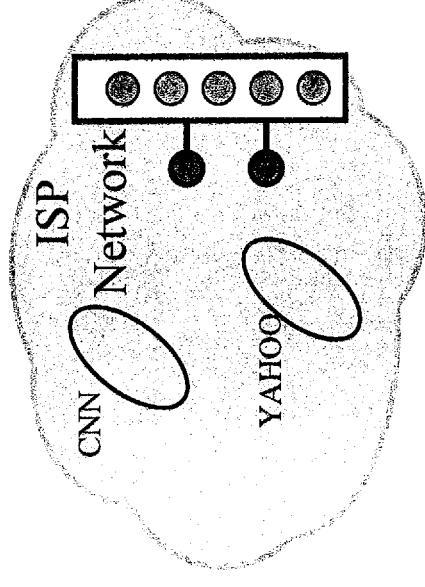
Marketing Servers Models

• Dist. Guard company



Guard ●

• Gatekeeper farms



Guard Architecture

